RAPPORT D'INSTALLATION SODECAF

MATHILDE NYAI / MARC LAPLAGNE

TABLE DES MATIERES

PRESENTATION DES SOUS RESEAU INTERNE DE L'ENTREPRISE 2

SOUS RESEAU COLLABORATEURS 2
SOUS RESEAU INFORMATIQUE 2
SOUS RESEAU EXPERTS 2
SOUS RESEAU VISITEURS 2
SCHEMA 3

CONFIGURATION DU ROUTEUR CISCO-TEAM23 3

MISE EN PLACE D'UN MOT DE PASSE CHIFFRE 3
MISE EN PLACE D'UN ACCES SSH 3
DEFINIR LE NOM DE D'HOTE ET DE DOMAINE 3
GENERER LES CLES RSA 3
ACTIVER LE PROTOCOLE SSH 4
ROUTES 4
SOUS INTERFACE 4
SOUS INTERFACE COLLABORATEURS 4
SOUS INTERFACE INFORMATIQUE 4
SOUS INTERFACE EXPERTS 4
SOUS INTERFACE VISITEURS 4
ACCESS-LIST 4
ACCESS-LIST COLLABORATEURS 4
ACCESS-LIST INFORMATIQUE 6
ACCESS-LIST EXPERTS 6
ACCESS-LIST VIVISTEURS 7
ACCESS-LIST 101 7

CONFIGURATION DU SWITCH 7

MISE EN PLACE D'UN MOT DE PASSE CHIFFRE 7
MISE EN PLACE D'UN ACCES SSH 7

DEFINIR LE NOM DE D'HOTE ET DE DOMAINE 8
GENERER LES CLES RSA 8
ACTIVER LE PROTOCOLE SSH 8
CREATION DES VLANS 8
CONFIGURATION DES INTERFACES 8

PRESENTATION DES SOUS RESEAU INTERNE DE L'ENTREPRISE

SOUS RESEAU COLLABORATEURS

172.23.1.0/27

Passerelle 172.23.1.30

Serveur DNS 172.16.23.1

SOUS RESEAU INFORMATIQUE

172.23.1.64/28

Passerelle 172.23.1.78

Serveur DNS 172.16.23.1

SOUS RESEAU EXPERTS

172.23.1.32/27

Passerelle 172.23.1.62

Serveur DNS 172.16.23.1

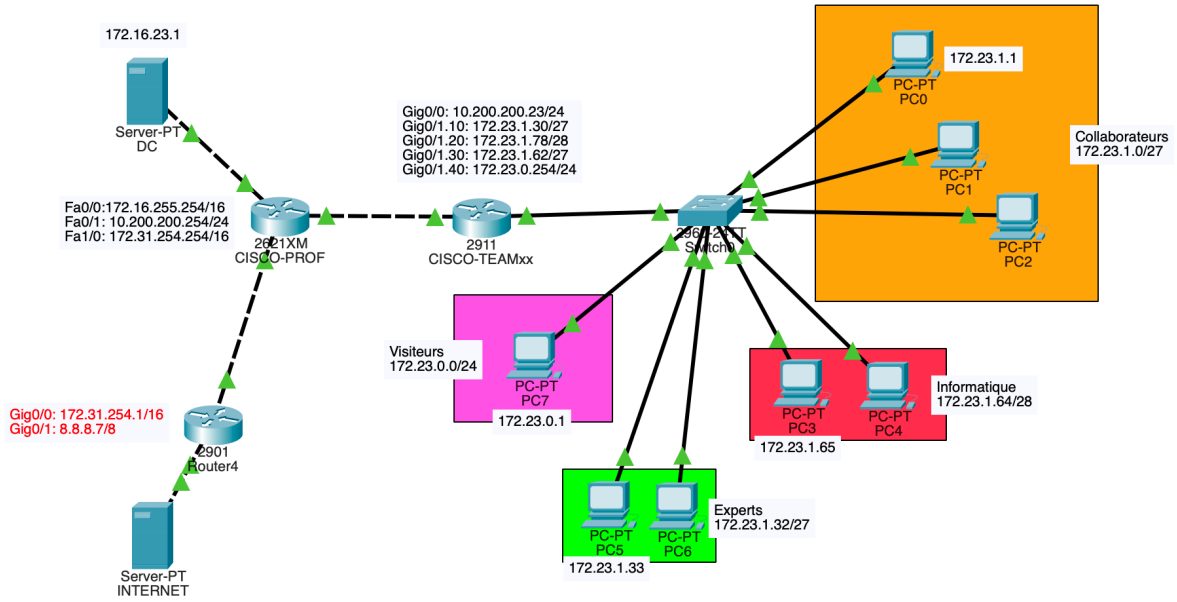
SOUS RESEAU VISITEURS

172.23.0.0/24

Passerelle 172.23.0.254

Serveur DNS 172.16.23.1

SCHEMA



CONFIGURATION DU ROUTEUR CISCO-TEAM23

MISE EN PLACE D'UN MOT DE PASSE CHIFFRE

enable
conf t
enable secret cJEFRh^mp#o&f8FEE
exit
write memory

MISE EN PLACE D'UN ACCES SSH

DEFINIR LE NOM DE D'HOTE ET DE DOMAINE

conf t
hostname CISCO-TEAM23
ip domain-name sodecaf.fr

GENERER LES CLES RSA

crypto key generate rsa

1024

ACTIVER LE PROTOCOLE SSH

```
ip ssh version 2
line vty 0 4
transport input ssh
login local
username team23 password $$V@8a11TtGw%H
write memory
```

ROUTES

ip route 0.0.0.0 0.0.0.0 10.200.200.254 => Route par défaut pour accéder aux autres réseaux

SOUS INTERFACE

SOUS INTERFACE COLLABORATEURS

```
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.23.1.30 255.255.255.224
 no shutdown
exit
```

SOUS INTERFACE INFORMATIQUE

```
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.23.1.78 255.255.255.240
 no shutdown
exit
```

SOUS INTERFACE EXPERTS

```
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 172.23.1.62 255.255.255.224
 no shutdown
exit
```

SOUS INTERFACE VISITEURS

```
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 172.23.0.254 255.255.255.0
 no shutdown
exit
```

ACCESS-LIST

ACCESS-LIST COLLABORATEURS

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 80 (HTTP)

access-list 110 permit tcp any gt 1023 any eq 80

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 443 (HTTPS)

access-list 110 permit tcp any gt 1023 any eq 443

Autoriser le protocole udp en provenance de toutes les machines collaborateurs, à destination du serveur DNS de l'entreprise situé sur l'IP 172.16.23.1

access-list 110 permit udp any host 172.16.23.1 eq 53

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination du serveur web de l'entreprise situé sur l'IP 172.16.23.1

access-list 110 permit tcp any gt 1023 host 172.16.23.1 eq 80

Autoriser les réponses du protocole icmp en provenance de toutes les machines collaborateurs, à destination du réseau Informatique de l'entreprise

access-list 110 permit icmp any 172.23.1.64 0.0.0.15 echo-reply

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 25 (SMTP)

access-list 110 permit tcp any any eq 25

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 143 (IMAP)

access-list 110 permit tcp any any eq 143

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 587 (SMTPS)

access-list 110 permit tcp any any eq 587

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 995 (POP3S)

access-list 110 permit tcp any any eq 995

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 993 (IMAPS)

access-list 110 permit tcp any any eq 993

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 110 (POP3)

access-list 110 permit tcp any any eq 110

Autoriser le protocole udp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 443 (Protocole UDP nécessaire pour Teams)

access-list 110 permit udp any any eq 443

Autoriser le protocole udp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 3482 (Teams)

access-list 110 permit udp any any eq 3481

Autoriser le protocole udp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur les ports supérieur à 50000 (Discord)

access-list 110 permit udp any any gt 50000

Interdire le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 20 et 21 (FTP)

access-list 110 deny tcp any any eq 20
access-list 110 deny tcp any any eq 21

int gig0/1.10
ip access-group 110 in
exit

ACCESS-LIST INFORMATIQUE

Accès à tous les PC du réseau

access-list 20 permit 172.23.1.64 0.0.0.15

int gig0/1.20
ip access-group 20 in
exit

ACCESS-LIST EXPERTS

access-list 130 permit tcp any gt 1023 any eq 80
access-list 130 permit tcp any gt 1023 any eq 443
access-list 130 permit udp any host 172.16.23.1 eq 53
access-list 130 permit tcp any gt 1023 host 172.16.23.1 eq 80
access-list 130 permit icmp any 172.23.1.64 0.0.0.15 echo-reply
access-list 130 permit tcp any any eq 25
access-list 130 permit tcp any any eq 143
access-list 130 permit tcp any any eq 587
access-list 130 permit tcp any any eq 995
access-list 130 permit tcp any any eq 993
access-list 130 permit tcp any any eq 110
access-list 130 permit udp any any eq 443
access-list 130 permit udp any any eq 3481
access-list 130 permit udp any any gt 50000

Autoriser le protocole tcp en provenance de toutes les machines collaborateurs, à destination de tous les postes sur le port 20 et 21 (FTP)

access-list 130 permit tcp any any eq 20
access-list 130 permit tcp any any eq 21

int gig0/1.30

ip access-group 130 in
exit

ACCESS-LIST VIVISTEURS

access-list 140 permit tcp any gt 1023 any eq 80
access-list 140 permit tcp any gt 1023 any eq 443
access-list 140 permit icmp any 172.23.1.64 0.0.0.15 echo-reply
access-list 140 permit tcp any any eq 25
access-list 140 permit tcp any any eq 143
access-list 140 permit tcp any any eq 587
access-list 140 permit tcp any any eq 995
access-list 140 permit tcp any any eq 993
access-list 140 permit tcp any any eq 110
access-list 140 permit udp any any eq 443
access-list 140 permit udp any any eq 3481
access-list 140 permit udp any any gt 50000
access-list 140 deny tcp any any eq 20
access-list 140 deny tcp any any eq 21

int gig0/1.40
ip access-group 140 in
exit

ACCESS-LIST 101

Autoriser seulement les protocoles 80, 443 et 53 en cas de connexion déjà établie

access-list 101 permit tcp any eq 80 any gt 1023 established
access-list 101 permit tcp any eq 443 any gt 1023 established
access-list 101 permit udp host 172.16.23.1 eq 53 any gt 1023

Autoriser les réponses au protocoles ICMP provenant de tous le postes, a destination du réseau Informatique de l'entreprise

access-list 101 permit icmp any 172.23.1.64 0.0.0.15 echo-reply

int gi0/0
ip access-group 101 in
exit

CONFIGURATION DU SWITCH

MISE EN PLACE D'UN MOT DE PASSE CHIFFRE

enable
conf t
enable secret cORh^mp#o&f7FE
exit
write memory

MISE EN PLACE D'UN ACCES SSH

DEFINIR LE NOM DE D'HOTE ET DE DOMAINE

```
conf t
hostname CISCO-TEAM23
ip domain-name sodecaf.fr
```

GENERER LES CLES RSA

```
crypto key generate rsa

1024
```

ACTIVER LE PROTOCOLE SSH

```
ip ssh version 2
line vty 0 4
transport input ssh
login local
username team23 password $$V@8a61YtGw%H
write memory
```

CREATION DES VLANS

```
vlan 10
 name Collaborateurs
exit

vlan 20
 name Informatique
exit

vlan 30
 name Experts
exit

vlan 40
 name Visiteurs
exit
```

CONFIGURATION DES INTERFACES

```
interface range FastEthernet0/2-4
 switchport mode access
 switchport access vlan 10
exit

interface range FastEthernet0/5-6
 switchport mode access
 switchport access vlan 20
exit

interface range FastEthernet0/7-8
 switchport mode access
 switchport access vlan 30
exit

interface FastEthernet0/9
```

```
 switchport mode access
 switchport access vlan 40
exit

interface gig0/1
no sh
switchport mode trunk
switchport trunk allow vlan 10,20,30,40
exit
```